PCI DSS 3.1 and the Impact on Wi-Fi Security
PCI DSS 3.1 and the Impact on Wi-Fi Security

Given the complexities of satisfying PCI data security and compliance and ongoing high profile retail data breaches, the PCI Security Council determined that additional guidance was needed to provide retailers with more clarity into the intent and scope of the PCI data security requirements.

With the latest revision of PCI DSS v3.1, the PCI Security Council emphasized implementing security into business as usual activities and best practices for maintaining ongoing PCI compliance. Specific guidance was provided for many requirements to ensure that PCI audit is not the focal point of security initiatives but rather that merchants are building security process into daily operations.

An example is PCI Requirement 11.1 requiring merchants to test for presence of rogue wireless devices in the cardholder data environment (CDE). PCI DSS v3.1 provides additional clarification around PCI Requirement 11 and its sub requirements, including 11.1.

In prior versions of the PCI DSS, Requirement 11.1 was broadly and simply required merchants to conduct a quarterly scan of the network to identify rogue wireless access points in the CDE. Additional guidance provided in PCI DSS v2.0 suggested that merchants can satisfy this requirement using a visual inspection of the network, which in many cases turned this requirement from an “active” security initiative into merely a compliance checkmark, leaving networks and sensitive data vulnerable to attack.

Making matters worse, many merchants falsely believe that simply turning off Wi-Fi and scoping it out of their cardholder data environments exempts them from having to conduct regular vulnerability scanning for unauthorized wireless on the network.

According to the Verizon 2015 Data Breach Report, organizations continue to struggle with PCI Requirement 11. Verizon reported last year that among organizations that met 95% of the PCI DSS controls, more than half failed Requirement 11. Meanwhile, compliance with sub-requirement 11.1 fell 10% from a year earlier, with Verzon noting that organizations often fail this control because they falsely believe that they don’t need to scan for rogue wireless access points if they have chosen not to use in-scope wireless networks.

PCI DSS 3.1 Requirement 11.1 provides additional guidance around the methods used for rogue Wi-Fi scanning based on the size and complexity of the environment.

PCI v3.1 emphasizes that security is a continual process, not a snapshot in time compliance checkmark. The updated PCI standards specifically call out the difference between a small kiosk environment where a visual inspection for a rogue AP may be adequate to meet the intent of the requirement vs. a large retail environment where perhaps there are enough locations or the size of each location is such that visual inspection is not adequate. In this case, for medium to large retail organizations performing continuous rogue AP scanning with a strong WIPS is more appropriate to meet the intent of the 11.1 requirement, not just a quarterly or visual inspection.

In the case of visual inspections, in many cases the merchant may be asking an employee (GM, Manager, regional manager) to look around the environment to see what’s different. But these employees are not trained to identify malicious devices. APs have gotten so small and have been designed to blend in with their environment, frequently making them difficult to detect. Visual inspection in a small and controlled environment may be viable, but in a retail stores where multiple ports/connections to the network are available, automated scanning is the only way to ensure 24X7 security.

Mojo AirTight automatically inventories and classifies all wireless assets in the merchant’s network, including approved wireless access points and mobile client devices. This greatly simplifies mandatory inventory methods so you are not maintaining an inventory of mobile devices in a spreadsheet and can help define the scope for the PCI audit.

PCI DSS 3.1 Requirement 2.4 adds clarity for maintaining an inventory of system components that are in scope for PCI.

In order to accurately and efficiently define the scope of their networks for PCI compliance, it is recommended that retailers maintain an inventory of system components that make up the CDE. By identifying the key systems in the CDE, the merchant can assure that essential systems are protected and properly segmented for optimal security.

In the CDE, it’s important that mobile devices are protected and classified properly. This greatly simplifies mandatory inventory methods so you are maintaining an inventory of mobile devices and can help define the scope for the PCI audit.

PCI 3.1 Requirement 9.9 protects POS terminals and devices from tampering or substitution.

It’s important that mobile devices in the CDE associate to the wireless network specific to its location. If you are deploying mobile devices for store associates (including mobile POS), Mojo AirTight can automatically distinguish those from neighboring clients and access points in your airspace that are not sensitive devices - a critical feature when it comes to PCI and security compliance.
Mojo AirTight will maintain an inventory of your client devices and alert you when one of those devices goes missing or when a hacker tries to lure an approved device onto an unsecure Wi-Fi network where they can grab sensitive data from it.

Mojo AirTight provides automatic alerts when a mobile POS device is lost or stolen. This is done by identifying when a device is no longer on the network for a defined period of time. For instance, if a mobile POS gets regular software or application updates overnight, if a device is absent for over an hour, Mojo AirTight alerts security and IT personnel so that access to that network and CDE can quickly be revoked to eliminate potential security vulnerabilities before a catastrophic incident can occur.

**PCI DSS 3.1 Requirement 10.6 clarifies the intent and scope of the daily log review.**

Daily log reviews have been very tedious for retailers. PCI clarified that the focus should be on suspicious activity in the environment and actionable events and data from monitoring systems.

Mojo AirTight provides highly accurate alerts and is not prone to the high numbers of false positive alerts. SSL vulnerabilities are usually associated with other WIPS solutions, allowing administrators to focus on actionable events without having to sift through all the noise that logs can accumulate. This applies to rogue AP incidents and alerts on client devices that are lost or stolen. Mojo AirTight can also integrate with log correlation tools in place to monitor web and ecommerce environments and back end transaction processing servers.

**PCI DSS 3.1 designates SSL as insufficient for data security.**

In April 2015, the PCI Security Standards Council (PCI SSC) published a revision to the PCI Data Security Standard. PCI DSS Version 3.1 addresses vulnerabilities within the Secure Sockets Layer (SSL) encryption protocol that can put payment data at risk. The Council had determined that Secure Sockets Layer (SSL) v3.1 is no longer acceptable for data security due to inherent weaknesses in SSL protocol. Merchants are now required to implement Transport Layer Security (TLS) to ensure the networks are secure.

With respect to transactions over wireless networks, all Wi-Fi devices in the CDE must be protected with strong encryption per PCI Requirement 4.1.1 - “…use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.”

Mojo AirTight automatically detects open (non-encrypted) networks and is equipped to block these vulnerable connections before sensitive data is compromised.

**How to Leverage Technology to Lower the Barriers to Wireless Security.**

Compliance officers are rightly concerned about human factors which can often be the soft underbelly of any security policy.

To future-proof themselves against both inadvertent security lapses and malicious internal or external actions, merchants should consider solutions “behavior-based” security, which includes:

- Strong device behavioral analysis logic, since traditional signatures and threshold based security solutions can’t catch up with the evolving monitoring scenarios.
- Fast response time to threats, to tackle the new and optimized attack and policy violation triggers.

How should merchants determine whether a wireless PCI solution stands up to the test of security beyond checklist compliance?

- Is threat scanning 24×7 or is it only occasional spot scanning? PCI does not require 24×7 scanning, but continuous scanning is the best practice. Notably, the entire Target breach occurred over only 3 weeks – that is a much briefer period than a quarter.

- Does the scan merely serve up raw data to compliance officers or does it filter out genuine threats so they can be mitigated? With too many alarms, it’s natural to become desensitized, letting the human behavioral factors undermine your security and compliance posture.

- Is the solution capable of detecting all types of vulnerabilities? Can it identify various types of rogue APs? If it can only identify a few types of rogues (such as rogues with correlation between their wired and wireless MAC addresses – so called MAC adjacency), how can you trust that report since there could be unidentified rogue APs connected to the CDE among the large number of APs detected during the scan?

- Is the solution capable of automatically containing the identified vulnerabilities? Although automatic mitigation is not a PCI requirement, in large nationwide deployments, automatic containment is a requirement for security. Automatic containment reduces the window of vulnerability. Moreover, automatic containment has to occur without false alarms which can disrupt legitimate operations.

- Is the solution capable of full security operation at the store level without critical dependence on WAN links?

The answer to these critical questions will determine if merchants can be fully armed to protect themselves either during a compliance audit or against a legitimate wireless threat.
Protecting Your Brand is Important. Go Beyond the Check Mark

Wi-Fi services are table stakes in retail operations for both in store staff and guests. Mojo Networks’ customers can get secure Wi-Fi access and best of breed security in one network infrastructure without the expense of an overlay security solution.

Mojo AirTight goes beyond the PCI compliance “checkmark” to ensure that your sensitive payment card data is secure from wireless secure breaches. Mojo AirTight automates PCI wireless compliance scanning and reporting of rogue APs and other wireless threats that can put your data at risk. Automated threat containment ensures your network and data are secure at all times.

Mojo AirTight’s PCI scanning and remediation solutions offer a radically less expensive alternative to any competitive options available today. Walking around with a wireless analyzer for conducting scans is a time-consuming process, limited in scope, cannot scale for large premises and is cost prohibitive for multiple sites. Mojo AirTight is a convenient, comprehensive, and cost-effective solution for protecting sensitive payment card data and maintaining a strong PCI compliance posture.

**The Mojo AirTight solution includes:**

- Automated 24x7 intrusion detection and rogue AP scanning
- Ability to maintain an up-to-date wireless device inventory (recommended by the PCI SSC)
- Automatic blocking of Rogue APs and other wireless threats or hack attacks

- Highly accurate wireless threat and compliance violation alerts via email
- Location tracking capabilities identify the physical location of threat posing Wi-Fi devices
- Scheduled and on-demand PCI report generation and delivery to your inbox

---

**Uncompromised Security**

Recognized by Gartner and IDC as leaders in WiFi security, Mojo AirTight protects your WLAN from threats such as rogue APs, WPA2 vulnerabilities, and man-in-the-middle attacks.

Find out more at [mojonetworks.com/security](http://mojonetworks.com/security)

---

**About Mojo Networks, Inc.**

Mojo Networks is redefining the modern WiFi platform. Imagine the scalability to set up millions of access points with a few clicks, all from your smartphone. Envision an Internet experience that engages users with your business to drive results. Stay secure on the same WiFi cloud powering major brands and the highest levels of government. And enjoy the cost savings of a cloud-first solution without the pricey markup of proprietary hardware. Welcome to the era of prolific connectivity. Founded in 2003, Mojo Networks (formerly known as AirTight Networks), serves customers in the Fortune 500, Global 2000 and large carriers around the world. Request a free demo of Mojo Cloud Managed WiFi Platform at [www.mojonetworks.com](http://www.mojonetworks.com)